



FIȘA DISCIPLINEI
ANUL UNIVERSITAR 2023 - 2024

1. DATE DESPRE PROGRAM

1.1 Instituția de învățământ superior	UNIVERSITATEA DIN CRAIOVA
1.2 Facultatea	Facultatea de Automatică, Calculatoare și Electronică
1.3 Departamentul	Departamentul de Automatică și Electronică
1.4 Domeniul de studii	Ingineria sistemelor
1.5 Ciclul de studii ¹	Licență
1.6 Programul de studii (denumire/cod) ² /Calificarea	Automatică și informatică aplicată / L20602022010

2. DATE DESPRE DISCIPLINĂ

2.1 Denumirea disciplinei		Securitate digitală							
2.2 Titularul activităților de curs		Prof. dr. ing. Dorin ȘENDRESCU							
2.3 Titularul activităților aplicative		Asist. drd. ing. Oana Mihaela CIUCĂ-GHEORGHE							
2.4 Anul de studiu	3	2.5 Semestrul	6	2.6 Tipul disciplinei (conținut) ³	DS	2.7 Regimul disciplinei (obligativitate) ⁴	DO	2.8 Tipul de evaluare	E

3. TIMPUL TOTAL ESTIMAT (ore pe semestru al activităților didactice)

3.1 Număr de ore pe săptămână	4	din care: 3.2 curs	2	3.3 laborator	2
3.4 Total ore din planul de învățământ	56	din care: 3.5 curs	28	3.6 laborator	28
3.7 Distribuția fondului de timp					ore
▪ Studiul după manual, suport de curs, bibliografie și notițe					5
▪ Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					4
▪ Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					5
▪ Tutoriat					-
▪ Examinări					2
▪ Alte activități: consultații, cercuri studențești					3
Total ore activități individuale		19			
3.8 Total ore pe semestru ⁵		75			
3.9 Numărul de credite ⁶		3			

4. PRECONDIȚII (acolo unde este cazul)

4.1 de curriculum	Studentul trebuie să posede cunoștințe de specialitate dobândite la următoarele discipline: Programarea calculatoarelor și limbaje de programare, Algebră liniară, geometrie analitică și diferențială, Procesare de documente, Ingineria sistemelor de programe.
4.2 de competențe	Nu sunt necesare.

5. CONDIȚII (acolo unde este cazul)

5.1. de desfășurare a cursului	Predarea cursului se face folosind videoproiectorul. Pentru unele explicații și răspunsuri la întrebări din sală se folosește tabla. Se asigură suport de curs în format electronic și acces la documentații actualizate. Procesul de predare are următoarea structură: <ul style="list-style-type: none">▪ 80% prezentare teoretică, pe baza suportului de curs (slide-uri)▪ 20% activitate interactivă (discuții cu studenții)
5.2. de desfășurare a seminarului/laboratorului/proiectului	Laboratorul utilizează o rețea de calculatoare. Sunt implementați algoritmi de securizare a informației și configurate și testate soft-urile de protecție a calculatoarelor (antivirus și firewall).

6. COMPETENȚELE SPECIFICE ACUMULATE ⁷

Competențe profesionale	<p>Prin cunoștințele predate la curs, prin exemplele prezentate și prin aplicațiile practice efectuate în cadrul laboratorului, cursul „Tehnici de securizare a informației” contribuie la formarea competențelor profesionale:</p> <ul style="list-style-type: none"> ▪ C2: Operarea cu concepte fundamentale din știința calculatoarelor, tehnologia informației și comunicațiilor;
Competențe transversale	

7. OBIECTIVELE DISCIPLINEI (reieșind din grila competențelor specifice acumulate)

7.1 Obiectivul general al disciplinei	Contribuie la formarea viitorilor ingineri automatiști, specialiști în conducerea proceselor și informatică aplicată, asigurându-le cunoștințe în domeniul securizării informației. Sunt abordate concepte de bază utilizate în proiectarea și realizarea sistemelor de securizare a datelor.
7.2 Obiectivele specifice	Introducere în teoria securizării informației, tehnici de protecție a datelor: parole, criptare cu cheie simetrică și cu cheie publică, semnături digitale, configurare programe antivirus și firewall. Laboratorul are rolul de a fixa cunoștințele teoretice și de a permite înțelegerea mecanismelor de protecție a datelor prin aplicații practice.

8. CONȚINUTURI

8.1 Curs (unități de conținut)	Nr. ore	Metode de predare
1. Generalități 1.1. Probleme generale privind protecția și securitatea datelor. 1.2. Fixarea terminologiei; Tratarea specificității securității în context Internet.	2	Predarea cursului se face folosind videoproiectorul. - 80% prezentare teoretică, pe baza suportului de curs (slide-uri). - 20% activitate interactivă (discuții cu studenții) Materialele necesare vor fi puse la dispoziția studenților în format electronic și în formă tipărită.
2. Concepte și modele aritmetico-logice utilizate în tehnicile criptografice 2.1. Operații booleene; 2.2. Elemente de teoria numerelor; 2.3. Aritmetică modulară.	2	
3. Criptografie cu cheie secretă. Detalierea tehnicilor de criptografie simetrică. 3.1. DES (Data Encryption Standard); 3.2. Algoritmi de substituție; 3.3. Tehnica one-time-pad.	2	
4. Criptografie cu chei publice. 4.1. Descrierea metodei RSA (Rivest-Shamir-Aldeman) 4.2. Descrierea metodei ElGamal; 4.3. Descrierea metodei Rabin	4	
5. Funcții de dispersie (hash) utilizate în criptografie 5.1. Descrierea metodei MD5 (Message Digest) 5.2. Descrierea metodei SHA (Secure Hash Algorithm).	2	
6. Semnături digitale. 6.1. Domenii de utilizare; 6.2. Algoritmi de criptare utilizați în semnătura digitală.	2	
7. Protocoale de autentificare 7.1. Protocolul Diffie-Helman; 7.2. Notari electronici; 7.3. Sisteme de încredere 7.4. Protocolul și sistemul Kerberos	4	
8. Securitate în cadrul protocolului TCP/IP. 8.1. Structura unui firewall. 8.2. Funcțiile unui firewall	2	

9. Protocole la nivel de aplicație și aplicații securizate. 9.1. Protocolul SSH; 9.2. Protocolul SFTP; 9.3. Protocolul HTTPS 9.4. Protocolul SSL.	2	
10. Viruși informatici 10.1. Anatomie; 10.2. Clasificări; 10.3. Funcționalități; 10.4. Protecția antivirus	2	
11. Denial of service (Negarea utilizării serviciilor) 11.1 atacuri de tip denial of service (DoS); 11.2 atacuri de tip flooding (inundație); 11.3 atacuri de tip denial of service distribuit; 11.4 atacuri de tip reflector și de tip amplificator; 11.5 contramăsuri posibile la atacuri DoS	2	
12 Sisteme firewall și de prevenire a intruziunilor 12.1 necesitatea „zidurilor ignifuge” (firewall); 12.2 tipuri de firewall-uri; 12.3 arhitecturi de rețele și locația firewall-urilor; 12.4 sisteme de prevenire a intruziunilor	2	
Total	28 ore	
Bibliografie ⁸ 1. W Stallings, Cryptography and Network Security, second ed., Prentice-Hall, 1999 2. Cormen T. Leiserson C. Rivest R introducere în algoritmi. Computer press Agora, 1999. 3. Jursic A. Menezes A. Elliptic curves and Cryptography http://www.certicom.com/research/weccrypt.html WhitePaper 4. Patriciu V. Criptografie și securitatea rețelelor de calculatoare. Ed. Tehnică, 1994 5. *** Resurse Web plecând de la . (http://WilliamStallings.com/Security2e.html). 6. Ciprian Răcuciu, Aspecte privind secretizarea semnalelor video, A XXVI-a Sesiune de Comunicări Științifice cu Participare Internațională, Ed. Academia Tehnică Militară, București, 1995. 7. Ciprian Răcuciu, Considerații asupra algoritmilor de criptanaliză statistică, A XXX-a Sesiune de Comunicări Științifice cu Participare Internațională, Ed. Academia Tehnică Militară, București, 2003.		
8.2 Activități aplicative (subiecte/teme)	Nr. ore	Metode de predare
Prezentarea noțiunilor de aritmetică modulară	2	Efectuarea lucrărilor de laborator se face folosind machete și programe de simulare pe calculator. Sunt puse la dispoziția studenților platforme de laborator care conțin un breviar teoretic și modul de desfășurare al lucrării. Activități: ▪ 60% desfășurarea lucrării ▪ 40% interpretarea rezultatelor și discuții cu studenții
Inițiere în utilizarea librăriei criptografice OpenSSL	2	
Implementarea algoritmilor cu cheie secretă	4	
Implementarea algoritmilor cu cheie publică	4	
Familiarizarea cu algoritmi de determinare a valorii rezumat și cei de semnătură digitală (MD5, SHA1, DSA, DH)	4	
Implementarea unui algoritm de semnătură digitală	2	
familiarizarea cu o infrastructură cu cheie publică (certIFICATE digitale, autorități de certificare, autorități de înregistrare)	2	
Studierea și configurarea unui firewall	2	
Implementarea unui protocol de securitate	2	
Instalare, configurare și familiarizare cu utilitarul SNORT (sistem de detecție a intruziunilor)	2	
Exemplificare de viruși informatici și folosirea anti-virusurilor	2	
Total	28 ore	

Bibliografie⁸

1. Held G. - Comunicații de date, Editura Teora, București, 1998.
2. V. Patriciu, Criptografia și Securitatea Rețelelor de Calculatoare cu aplicații în C și Pascal, Ed. Tehnică, București, 1994.
3. H. Beker and F. Piper, Cipher Systems: The Protection of Communications, John Wiley & Sons, New York, 1982.
4. Bruce Schneier, Applied Cryptography, John Wiley & Sons, 1996.
5. Boca Raton, Cryptography: Theory and Practice, CRC Press, , Florida, 1995.

**9. COROBORAREA CONȚINUTURILOR DISCIPLINEI CU AȘTEPTĂRILE REPREZENTANȚILOR
COMUNITĂȚII EPISTEMICE, ASOCIAȚIILOR PROFESIONALE ȘI ANGAJATORI REPREZENTATIVI DIN
DOMENIUL AFERENT PROGRAMULUI**

Conținutul cursului a fost discutat cu reprezentanții:

- CS Romania
- Net Rom
- IT Six Global Services

10. EVALUARE

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	- Înțelegerea fundamentelor teoretice corespunzătoare securității informatice. - Capacitatea de a realiza conexiuni între noțiunile predate. - Capacitatea de analiză și sinteză într-o situație concretă.	Examen scris parțial Examen scris final	40% 40%
10.5 Activități aplicative Laborator	- Interpretarea rezultatelor; - Soluțiile aplicațiilor se prezintă și se discută în cadrul grupei	Verificare pe parcurs și testare finală	20%
10.6 Standard minim de performanță (volumul de cunoștințe minim necesar pentru promovarea disciplinei și modul în care se verifică stăpânirea lui)			
<ul style="list-style-type: none"> ▪ Obținerea a minim 50 % din punctajul verificărilor pe parcurs, testărilor de laborator și examenului final. ▪ Calculul notei finale se face prin rotunjirea la notă întreagă a punctajului final. 			

Data completării:

Titular curs
Prof. dr. ing. Dorin Șendrescu

Titular activități aplicative
Asist. dr. ing Oana Mihaela CIUCĂ-GHEORGHE

.....

.....

Data avizării în departament:

Director de departament
Prof. dr. ing. Cosmin IONETE

.....

Notă:

- 1) Ciclul de studii - se alege una din variantele: L (licență)/ M (master)/ D (doctorat).
- 2) Se înscrie codul prevăzut în HG nr. 493/17.07.2013.
- 3) Tip (conținut) - se alege una din variantele:
 - pentru nivelul de licență: DF (disciplină fundamentală)/ DD (disciplină din domeniu)/ DS (disciplină de specialitate)/ DC (disciplină complementară);
 - pentru nivelul de master: DA (disciplină de aprofundare)/ DS (disciplină de sinteză)/ DCA (disciplină de cunoaștere avansată).
- 4) Regimul disciplinei (obligativitate) - se alege una din variantele: DI (disciplină obligatorie)/ DO (disciplină opțională)/ FC (disciplină facultativă).
- 5) Se obține prin însumarea numărului de ore de la punctele 3.4 și 3.7.
- 6) Un credit este echivalent cu 25 – 30 de ore de studiu (activități didactice și studiu individual).
În cazul DAEM 1 pct. credit este egal cu 27 de ore de studiu.
- 7) Aspectul competențelor profesionale și competențelor transversale va fi tratat cf. Metodologiei OMECTS 5703/18.12.2011. Se vor prelua competențele care sunt precizate în Registrul Național al Calificărilor din Învățământul Superior RNCIS (http://www.rncis.ro/portal/page?_pageid=117.70218&_dad=portal&_schema=PORTAL) pentru domeniul de studiu de la pct. 1.4 și programul de studii de la pct. 1.6 din această fișă, la care participă disciplina.
- 8) Se recomandă ca cel puțin un titlu să aparțină colectivului disciplinei iar cel puțin 2-3 titluri să se refere la lucrări relevante pentru disciplină, de circulație națională și internațională, existente în biblioteca UCv.